**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Kazuhiko TAKABAYASHI et al.

International Application No.: PCT/JP2004/002113

International Filing Date: February 24, 2004

For: DEVICE-TO-DEVICE AUTHENTICATION SYSTEM, DEVICE-TO-DEVICE AUTHENTICATION METHOD, COMMUNICATION APPARATUS, AND COMPUTER PROGRAM

745 Fifth Avenue
New York, NY 10151

**EXPRESS MAIL**

Mailing Label Number: EV206809675US

Date of Deposit: January 10, 2005

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

**CLAIM OF PRIORITY UNDER 37 C.F.R. § 1.78(a)(2)**

Mail Stop PCT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 35 U.S.C. 119, this application is entitled to a claim of priority to Japan Application No. 2003-132902 filed 12 May 2003.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By:

William S. Frommer
Reg. No. 25,506
Tel. (212) 588-0800

# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　５月１２日

出願番号
Application Number: 特願２００３－１３２９０２

[ST. 10/C]: [ＪＰ２００３－１３２９０２]

出願人
Applicant(s): ソニー株式会社



２００４年　３月２６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０２５０６５

【書類名】　特許願
【整理番号】　0390411104
【提出日】　平成15年 5月12日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　高林　和彦
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　中野　雄彦
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　本田　康晃
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　五十嵐　卓也
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100093241
　【弁理士】
　【氏名又は名称】　宮田　正昭

【選任した代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【手数料の表示】

【予納台帳番号】　048747

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項１】

ネットワーク上の機器同士が一定の範囲内で接続されているどうかを認証する機器間認証システムであって、

前記ネットワーク経由で相互接続されている各機器は、仲介装置を着脱可能に物理アクセスする仲介装置インターフェースと、所定時間内に同じ仲介装置へ物理アクセスした他の機器をコンテンツを利用可能なローカル環境に置かれていると認証するローカル環境管理手段を備え、

ローカル環境内では機器間でコンテンツの利用が許可される、

ことを特徴とする機器間認証システム。

【請求項２】

一方の機器はコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

前記ローカル環境管理手段により双方の機器がローカル環境下に存在することが確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１に記載の機器間認証システム。

【請求項３】

前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能であり、

ホーム・サーバ毎に、同じホーム・ネットワーク上に存在することが確認されたクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１に記載の機器間認証システム。

【請求項４】

クライアントは、同じホーム・ネットワーク上の２台以上のホーム・サーバか

らコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、
ことを特徴とする請求項３に記載の機器間認証システム。

【請求項５】

クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、その以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、
ことを特徴とする請求項３に記載の機器間認証システム。

【請求項６】

前記仲介装置は所定の識別情報を保持することができ、

前記ローカル環境管理手段は、仲介装置に物理アクセスした各機器が仲介装置から同じ識別情報を読み取ったこと及び／又はそれぞれが識別情報を読み取った時刻が所定時間内であることを以って各機器がローカル環境に置かれていると認証する、
ことを特徴とする請求項１に記載の機器間認証システム。

【請求項７】

前記仲介装置は秘密情報を安全に保持するメモリを備え、

前記仲介装置に物理アクセスする機器の１つは秘密情報を生成することができ、

前記ローカル環境管理手段は、１つの機器が生成した秘密情報を前記仲介装置経由で他の機器が所定時間内に取得できたことを以って各機器がローカル環境に置かれていると認証する、
ことを特徴とする請求項１に記載の機器間認証システム。

【請求項８】

秘密情報を生成した機器は所定時間経過後に該秘密情報を消失し、

前記ローカル環境管理手段は、秘密情報を生成した機器において該秘密情報を消失する以前に該秘密情報を共有することができた機器をローカル環境に置かれていると認証する、

ことを特徴とする請求項７に記載の機器間認証システム。

【請求項９】

ネットワーク上の機器同士が一定の範囲内で接続されているどうかを認証する機器間認証方法であって、

前記ネットワーク経由で相互接続されている各機器は、仲介装置を着脱可能に物理アクセスする仲介装置インターフェースを備え、

所定時間内に同じ仲介装置へ物理アクセスした他の機器をコンテンツを利用可能なローカル環境に置かれていると認証するローカル環境管理ステップ、

ローカル環境内では機器間でコンテンツの利用が許可されるコンテンツ利用ステップと、

を具備することを特徴とする機器間認証方法。

【請求項１０】

一方の機器はコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

前記コンテンツ利用ステップでは、双方の機器がローカル環境下に存在することが確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項９に記載の機器間認証方法。

【請求項１１】

前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能であり、

前記コンテンツ利用ステップでは、ホーム・サーバ毎に、同じホーム・ネットワーク上に存在することが確認されたクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項９に記載の機器間認証方法。

【請求項１２】

前記コンテンツ利用ステップでは、クライアントは同じホーム・ネットワーク上の２台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項１１に記載の機器間認証方法。

【請求項１３】

前記コンテンツ利用ステップでは、クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、その以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

ことを特徴とする請求項１１に記載の機器間認証方法。

【請求項１４】

前記仲介装置は所定の識別情報を保持することができ、

前記ローカル環境管理ステップでは、仲介装置に物理アクセスした各機器が仲介装置から同じ識別情報を読み取ったこと及び／又はそれぞれが識別情報を読み取った時刻が所定時間内であることを以って各機器がローカル環境に置かれていると認証する、

ことを特徴とする請求項９に記載の機器間認証方法。

【請求項１５】

前記仲介装置は秘密情報を安全に保持するメモリを備え、

前記仲介装置に物理アクセスする機器の１つは秘密情報を生成することができ、

前記ローカル環境管理ステップでは、１つの機器が生成した秘密情報を前記仲介装置経由で他の機器が所定時間内に取得できたことを以って各機器がローカル環境に置かれていると認証する、

ことを特徴とする請求項９に記載の機器間認証方法。

【請求項１６】

秘密情報を生成した機器は所定時間経過後に該秘密情報を消失し、

前記ローカル環境管理ステップでは、秘密情報を生成した機器において該秘密情報を消失する以前に該秘密情報を共有することができた機器をローカル環境に置かれていると認証する、

ことを特徴とする請求項１５に記載の機器間認証方法。

【請求項１７】

ネットワーク上で所定の許容範囲内でコンテンツを利用する通信機器であって、

仲介装置を着脱可能に物理アクセスする仲介装置インターフェースと、

所定時間内に同じ仲介装置へ物理アクセスした他の機器をコンテンツを利用可能なローカル環境に置かれていると認証するローカル環境管理手段と、

ローカル環境内でコンテンツを正当に利用するコンテンツ利用手段と、

を具備することを特徴とする通信機器。

【請求項１８】

前記ネットワーク上でコンテンツを提供するホーム・サーバとして動作し、

前記コンテンツ利用手段は、前記ローカル環境管理手段により同じローカル環境に存在することが確認された機器に対してのみコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項１７に記載の通信機器。

【請求項１９】

前記ネットワーク上でホーム・サーバに対してコンテンツを要求するクライアントとして動作し、

前記コンテンツ利用手段は、前記ローカル環境管理手段により同じローカル環境に存在することが確認されたホーム・サーバからのみコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受ける、

ことを特徴とする請求項１７に記載の通信機器。

【請求項２０】

前記ローカル環境下には２台以上のホーム・サーバを設置可能であり、

前記コンテンツ利用手段は、前記ローカル環境管理手段により同じローカル環境に存在することが確認された２台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項１９に記載の通信機器。

【請求項２１】

前記コンテンツ利用手段は、同じローカル環境下の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム

・サーバに接続した時点で、その以外のローカル環境のホーム・サーバから取得したコンテンツを利用不能となる、
ことを特徴とする請求項１９に記載の通信機器。

【請求項２２】

仲介装置は所定の識別情報を保持することができ、

前記仲介装置インターフェースは、仲介装置が物理アクセスしたことに応答して識別情報を読み取り、

前記ローカル環境管理手段は、仲介装置から読み取った識別情報が同じであり、及び／又は、識別情報を読み取った時刻が所定時間内である機器を自己のローカル環境に置かれていると認証する、
ことを特徴とする請求項１７に記載の通信機器。

【請求項２３】

前記仲介装置は秘密情報を安全に保持するメモリを備え、

前記通信機器は秘密情報を生成する秘密情報生成装置をさらに備え、

前記仲介装置インターフェースは、仲介装置が物理アクセスしたことに応答して秘密情報を該仲介装置内のメモリに書き込み、

前記ローカル環境管理手段は、自己の生成した秘密情報を前記仲介装置経由で他の機器が所定時間内に取得できたことを以って該他の機器が自己のローカル環境に置かれていると認証する、
ことを特徴とする請求項１７に記載の通信機器。

【請求項２４】

前記仲介装置は秘密情報を安全に保持するメモリを備え、

前記仲介装置インターフェースは、仲介装置が物理アクセスしたことに応答して秘密情報を該仲介装置内のメモリから秘密情報を取り出し、

前記ローカル環境管理手段は、仲介装置から読み取った秘密情報が同じであり、及び／又は、秘密情報を読み取った時刻が所定時間内である機器を自己のローカル環境に置かれていると認証する、
ことを特徴とする請求項２３に記載の通信機器。

【請求項２５】

秘密情報は生成されてから所定時間経過後に消失し、

前記ローカル環境管理手段は、秘密情報を消失する以前に該秘密情報を共有することができた機器をローカル環境に置かれていると認証する、

ことを特徴とする請求項２３に記載の通信機器。

【請求項２６】

ネットワーク上の機器同士が一定の範囲内で接続されているどうかを認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

前記ネットワーク経由で相互接続されている各機器は、仲介装置を着脱可能に物理アクセスする仲介装置インターフェースを備え、

所定時間内に同じ仲介装置へ物理アクセスした他の機器をコンテンツを利用可能なローカル環境に置かれていると認証するローカル環境管理ステップ、

ローカル環境内では機器間でコンテンツの利用が許可されるコンテンツ利用ステップと、

を具備することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク経由で接続される機器同士の真正性を認証する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに係り、特に、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で接続される機器同士の真正性を認証する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに関する。

【０００２】

さらに詳しくは、本発明は、機器同士が一定の範囲内で接続されているどうかを認証する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに係り、特に、一方の機器において正当に取得されているコンテンツを他方の機器が著作権法で認められる私的使用の範囲内で利用できるかどうかを認証する機器間認証システム及び機器間認証方法、通信装置、並びにコン

ピュータ・プログラムに関する。

【０００３】

【従来の技術】

近年のインターネットの普及により、コンピュータ・ファイルを始めとした各種のデジタル・コンテンツをネットワーク配信することが盛んに行なわれている。また、広帯域通信網（ｘＤＳＬ（ｘ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎｅ）、ＣＡＴＶ（Ｃａｂｌｅ　ＴＶ）、無線ネットワークなど）の普及により、音楽データや画像データ、電子出版物などのデジタル・データや、さらには動画像などリッチ・コンテンツの配信もユーザにストレスなく伝送できるような仕組みが整いつつある。

【０００４】

一方、配信されるコンテンツはデジタル・データであり、コピーや改竄などの不正な操作を比較的容易に行なうことができる。また、現在これらのコンテンツのコピーや改竄などの不正行為は頻繁に行なわれており、これがデジタル・コンテンツ・ベンダの利益を阻害する主要な要因となっている。この結果、コンテンツの値段も高くしなければならなくなり、普及の障壁となるという悪循環が起こっている。

【０００５】

例えば、最近では一般家庭内にもコンピュータやネットワークなどの技術が深く浸透してきている。家庭内のパーソナル・コンピュータやＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）などの情報機器、さらにはテレビ受像機やビデオ再生装置などの各種の情報家電がホーム・ネットワーク経由で相互接続されている。また、このようなホーム・ネットワークは、多くの場合、ルータ経由でインターネットを始めとする外部の広域ネットワークに相互接続されている。そして、インターネット上のサーバから正当に取得されたコンテンツは、ホーム・ネットワーク上のサーバ（以下、「ホーム・サーバ」とも呼ぶ）に蓄積された後、家庭内の他の端末（クライアント）へホーム・ネットワーク経由で配信される。

【０００６】

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに順ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている（著作権法第３０条を参照のこと）。

【０００７】

この私的使用の範囲を上述したホーム・ネットワークにおいて適用した場合、ホーム・ネットワークに接続されているクライアント端末は、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される（勿論、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある）。

【０００８】

しかしながら、ホーム・ネットワーク上にログインしたクライアント端末が私的使用の範囲にあるかどうかを識別することは、現状の技術では困難である。

【０００９】

例えば、ホーム・ネットワークはルータを介して外部のネットワークとＩＰプロトコル・ベースで相互接続されていることから、ホーム・サーバにとってはアクセスしてきたクライアントが実際にどこにいるのかは不明である。外部（遠隔）からのアクセスに対しホーム・サーバがコンテンツを提供してしまうと、コンテンツの利用はほぼ無制限となってしまい、コンテンツに関する著作権は保護されないに等しい。この結果、コンテンツ製作者は創作意欲を失いかねない。

【００１０】

また、ホーム・サーバがホーム・ネットワーク内のクライアント端末に対して一様にコンテンツの利用を許可した場合、同じクライアント端末が時間差をおいて複数のホーム・ネットワークに跨ってログインすることにより、ほぼ無尽蔵にコンテンツを利用することが可能となってしまう。

【００１１】

他方、クライアント端末に対して厳しい制限を課してしまうと、ユーザは、本

来著作権法上で認められている私的使用を確保することができなくなってしまう。この結果、ユーザがコンテンツを十分に享受することができず、ホーム・サーバやコンテンツ配信サービスの利用が進まないために、コンテンツ事業の発展自体を阻害しかねない。

【００１２】

例えば、著作物を正規に購入した利用者に自由利用が認められているということに鑑み、利用者がネットワーク上での情報を複製して利用するにあたって、コンテンツの権利保持者の理解が得られ易い方法に関する提案がなされている（例えば、特許文献１を参照のこと）。しかしながら、これは利用者を情報の利用権保持者との関係レベルによって分類し、関係レベル毎に異なる配信方法で情報を配信するというもので、ネットワーク上のどこまでが私的使用の範囲に該当するのかを識別するものではない。

【００１３】

現在、ホーム・ネットワークを構成するプロトコルとして、例えばＵＰｎＰ（Ｕｎｉｖｅｒｓａｌ　Ｐｌｕｇ　ａｎｄ　Ｐｌａｙ）が知られている。ＵＰｎＰによれば、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり、ネットワーク接続された機器間では困難な操作や設定を伴うことなくコンテンツ提供サービスを行なうことが可能となる。また、ＵＰｎＰは、オペレーティング・システム（ＯＳ）に非依存であり、容易に機器の追加ができるという利点を持つ。

【００１４】

ＵＰｎＰでは、ネットワーク接続された機器間で、ＸＭＬ（ｅＸｔｅｎｄｅｄ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）形式で記述された定義ファイルを交換して相互認証を行なう。ＵＰｎＰの処理の概要は以下の通りである。

【００１５】

（１）アドレッシング処理：ＩＰアドレスなどの自己のデバイスＩＤを取得する

（２）ディスカバリ処理：ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する

（３）サービス要求処理：ディスカバリ処理で取得された情報に基づいて各デバ

イスにサービスを要求する

【００１６】

このような処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供並びに受領が可能となる。新たにネットワークに接続される機器は、アドレッシング処理によりデバイスＩＤを取得し、ディスカバリ処理によりネットワーク接続されている他のデバイスの情報を取得し、サービス要求が可能となる。

【００１７】

ホーム・サーバに格納されたコンテンツは、ホーム・ネットワーク上の他の機器からアクセス可能となる。例えば、ＵＰｎＰ接続を実行した機器によってコンテンツを取得することが可能である。コンテンツが映像データや音声データの場合、ネットワーク接続機器として、ＴＶやプレーヤなどを接続すれば、映画や音楽を視聴することができる。

【００１８】

しかし、ホーム・ネットワーク内の機器、例えばホーム・サーバには私的なコンテンツや有料コンテンツなど著作権管理を要求されるコンテンツが格納されていることから、不正アクセスの対策を考慮する必要がある。

【００１９】

コンテンツの利用権（ライセンス）を有するユーザの機器によるアクセスは許容されて当然である。しかしながら、ホーム・ルータ経由で外部ネットワークに相互接続されているホーム・ネットワーク環境では、ライセンスを持たないユーザがホーム・ネットワークに入り込むことも可能である。

【００２０】

不正アクセスを排除するため、例えば、ホーム・サーバにアクセスを許容するクライアントのリストを保持させ、クライアントからホーム・サーバへのアクセス要求が行なわれる度に、リストとの照合処理を実行して、不正アクセスを排除することができる。

【００２１】

例えば、各通信機器に固有の物理アドレスであるＭＡＣ（Ｍｅｄｉａ　Ａｃｃ

ｅｓｓ Ｃｏｎｔｒｏｌ）アドレスを用いてアクセス許容機器リストとして設定するＭＡＣアドレス・フィルタリングが知られている。すなわち、ホーム・ネットワークのような内部ネットワークと外部ネットワークとを隔離するルータ又はゲートウェイにアクセスを許容する各機器のＭＡＣアドレスを登録しておき、受信したパケットに付されているＭＡＣアドレスと登録されたＭＡＣアドレスとを照合し、未登録のＭＡＣアドレスを持つ機器からのアクセスを拒否する（例えば、特許文献２を参照のこと）。

【００２２】

しかしながら、アクセス許容機器リストを構築するためには、内部ネットワークに接続されるすべての機器のＭＡＣアドレスを調べる必要があり、また、取得したすべてのＭＡＣアドレスを入力してリストを作成する手間が必要である。また、ホーム・ネットワークにおいては、接続される機器が比較的頻繁に変更され、かかる変更の度にアクセス許容機器リストを修正しなければならない。

【００２３】

【特許文献１】

特開２００２－７３８６１号公報

【特許文献２】

特開平１０－２７１１５４号公報

【００２４】

【発明が解決しようとする課題】

本発明の目的は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で接続される機器同士の真正性を好適に認証することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することにある。

【００２５】

本発明のさらなる目的は、一方の機器において正当に取得されているコンテンツを他方の機器が著作権法で認められる私的使用の範囲内で利用できるかどうかを好適に認証することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することにある。

【００２６】

【課題を解決するための手段及び作用】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、ネットワーク上の機器同士が一定の範囲内で接続されているどうかを認証する機器間認証システムであって、

前記ネットワーク経由で相互接続されている各機器は、仲介装置を着脱可能に物理アクセスする仲介装置インターフェースと、所定時間内に同じ仲介装置へ物理アクセスした他の機器をコンテンツを利用可能なローカル環境に置かれていると認証するローカル環境管理手段を備え、

ローカル環境内では機器間でコンテンツの利用が許可される、

ことを特徴とする機器間認証システムである。

【００２７】

但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュールが単一の筐体内にあるか否かは特に問わない。

【００２８】

ホーム・ネットワークに接続される一方の機器はホーム・サーバであり、前記ルータ経由で外部ネットワークから、あるいはパッケージ・メディアや放送受信を介してコンテンツを正当に取得する。また、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントである。そして、双方の機器が同じホーム・ネットワーク上に存在することが確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう。

【００２９】

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに順ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている。

【００３０】

そこで、本発明では、仲介装置を所定時間内に物理的に交換することができる程度の至近距離すなわちローカル環境に存在するクライアント端末は、私的な使用の範囲内にあるという前提に立ち、ローカル環境管理手段によりローカル環境下にあることが認証されたクライアントに限り、ホーム・サーバ上に蓄積されているコンテンツを利用することができるようにした。

【００３１】

前記ホーム・ネットワーク上には２台以上のホーム・サーバを設置可能である。このような場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、それぞれ独自にこれらをメンバー登録してグループを形成し、コンテンツ配信並びコンテンツ使用のライセンスを発行する。さらに、クライアント端末は、同じホーム・ネットワーク上の２台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

【００３２】

この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるから、ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当である。

【００３３】

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、時間差をおいて、複数のホーム・ネットワークに跨って複数のホーム・サーバのグループに所属することまでは認めるべきでない。別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しいからである。

【００３４】

したがって、クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク

上のホーム・サーバに接続した時点で、その以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる。

【００３５】

現状のネットワーク・プロトコルでは、ネットワーク経由で相互接続されている機器同士が真正すなわち個人的又は家庭の範囲内でコンテンツを私的使用できるかどうかを識別する仕組みは提供されていない。そこで、本発明では、ホーム・ネットワーク上に接続されている機器は、家庭内すなわち至近距離に位置し、ユーザは比較的短い時間のうちに互いの機器に物理的にアクセスすることができることを鑑み、ローカル環境管理手段は、互いの機器が短い時間内で同じ物理媒体へのアクセスを共有することができたかどうかにより、同じローカル環境下に存在しているかどうかを識別するようにした。

【００３６】

例えば、所定の識別情報を保持することができる仲介装置を適用した場合、前記ローカル環境管理手段は、仲介装置に物理アクセスした各機器が仲介装置から同じ識別情報を読み取ったこと及び／又はそれぞれが識別情報を読み取った時刻が所定時間内であることを以って各機器がローカル環境に置かれていると認証することができる。

【００３７】

また、秘密情報を安全に保持する耐タンパ性のあるメモリを備えた仲介装置を適用した場合、少なくとも１つの機器が乱数あるいはその他の形態の秘密情報を生成する機能を搭載し、前記ローカル環境管理手段は、１つの機器が生成した秘密情報を前記仲介装置経由で他の機器が所定時間内に取得できたことを以って各機器がローカル環境に置かれていると認証することができる。

【００３８】

このとき、秘密情報を生成した機器は所定時間経過後に該秘密情報を消失するようにしてもよい。この場合、前記ローカル環境管理手段は、秘密情報を生成した機器において該秘密情報を消失する以前に該秘密情報を共有することができた機器をローカル環境に置かれていると認証することができる。

【００３９】

また、本発明の第２の側面は、ネットワーク上の機器同士が一定の範囲内で接続されているどうかを認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

前記ネットワーク経由で相互接続されている各機器は、仲介装置を着脱可能に物理アクセスする仲介装置インターフェースを備え、

所定時間内に同じ仲介装置へ物理アクセスした他の機器をコンテンツを利用可能なローカル環境に置かれていると認証するローカル環境管理ステップ、

ローカル環境内では機器間でコンテンツの利用が許可されるコンテンツ利用ステップと、

を具備することを特徴とするコンピュータ・プログラムである。

【００４０】

本発明の第２の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第２の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１の側面に係る機器間認証システムと同様の作用効果を得ることができる。

【００４１】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４２】

【発明の実施の形態】

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに順ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている（著作権法第３０条を参照のこと）。

【００４３】

本発明者らは、ホーム・ネットワーク内（以下、「ローカル環境」とも呼ぶ）のクライアント端末は、私的な使用の範囲内にあるという前提に立ち、ローカル環境下のクライアントに限り、ホーム・サーバ上に蓄積されているコンテンツを利用することができるというシステムを提案する。

【００４４】

ここで、ローカル環境の定義について説明しておく。

【００４５】

図１には、ホーム・ネットワークの基本構成を模式的に示している。同図に示すように、家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどの外部ネットワークに接続されている。

【００４６】

ホーム・ネットワーク上には、ホーム・サーバと、１以上のクライアント端末が存在する。ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを取得し、蓄積し、家庭内でコンテンツを配信する。勿論、ホーム・サーバは、パッケージ・メディアや放送受信など、ネットワーク以外の手段により、コンテンツを取得することができる。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用する。

【００４７】

ホーム・ネットワークに接続されているクライアント端末は、ローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される。

【００４８】

そこで、ホーム・サーバは、ローカル環境下のこれらクライアント端末をメンバー登録し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。勿論、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある。

【００４９】

ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを

取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

【００５０】

一方、ホーム・ネットワーク上に存在しない、すなわちリモート環境のクライアント端末は、個人的又は家庭の範囲内での使用であるとは考えられない。リモート環境のクライアント端末にコンテンツの利用を認めると、コンテンツの利用はほぼ無制限となってしまい、コンテンツに関する著作権は保護されないに等しくなるからである。そこで、ホーム・サーバは、リモート環境のクライアントをメンバーとして登録せず、また、コンテンツのライセンスを発行しない。

【００５１】

図１に示した例では、ホーム・ネットワーク上には１つのホーム・サーバしか存在しないが、勿論、２以上のホーム・サーバを同じホーム・サーバ上に設置して、各ホーム・サーバがホーム・ネットワーク内でそれぞれ独自にコンテンツの配信サービスを行なうようにしてもよい。

【００５２】

図２には、２台のホーム・サーバが存在するホーム・ネットワークの構成例を示している。

【００５３】

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、これらをメンバー登録してグループを形成し、コンテンツ配信並びコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

【００５４】

さらに、クライアント端末は、同じホーム・ネットワーク上の２台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し

、個人的又は家庭の範囲内での使用であると推定されるから、ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当であると思料される。

【００５５】

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、複数のホーム・ネットワークに跨って複数のホーム・サーバのグループに所属することまでは認めるべきでない（図３を参照のこと）。

【００５６】

別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しい。ローカル環境が個人的又は家庭の範囲内であるのに対し、リモート環境は個人的又は家庭の範囲を逸脱する。

【００５７】

クライアント端末が時間差をかけて複数のホーム・ネットワークに跨って接続することは技術的には可能であるが、これに併せてコンテンツの利用を逐次許可していくと、コンテンツの利用はほぼ無制限となってしまい、コンテンツに関する著作権は保護されないに等しくなる。

【００５８】

以上を総括すると、ホーム・ネットワーク上において、個人的又は家庭の範囲内での使用であると推定されるローカル環境を実現するためには、以下の事柄が必要条件であることが導出される。

【００５９】

（１）ホーム・サーバは、ホーム・ネットワーク外からのメンバー登録を認めない。

（２）同じホーム・ネットワーク内に２台以上のホーム・サーバがあるときには、ホーム・サーバ毎にメンバー登録、グループ管理を行なう。ホーム・ネットワーク上の各クライアントは２以上のホーム・サーバに登録することができる。但

し、同時登録されるホーム・サーバは同じホーム・ネットワークに存在しなければならない。

【００６０】

このようなローカル環境を実現するためには、ホーム・サーバとクライアント端末間で、お互い同じホーム・ネットワーク上に存在するかどうかを識別する仕組みが必要となる。

【００６１】

現状のネットワーク・プロトコルでは、ホーム・ネットワークなどネットワークをセグメント単位で識別する仕組みは提供されていない。そこで、本発明者らは、ホーム・ネットワーク上に接続されている機器は、家庭内すなわち至近距離に位置し、ユーザは比較的短い時間のうちに互いの機器に物理的にアクセスすることができることを鑑み、コンテンツを配信するホーム・サーバとコンテンツを利用するクライアント端末が短い時間内で同じ物理媒体へのアクセスを共有することができたかどうかにより、同じホーム・ネットワークに接続されているかどうかを識別する方法を提案する。

【００６２】

ここで言う、短時間のうちに２つの機器で発生する物理的なアクセスには、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）やメモリ・スティックなどの標準的にインターフェースを介して機器へ装着される記憶媒体の挿抜、非接触ＩＣカードに対する読み書き動作を利用することができる。あるいは、ＩｒＤＡなどの近距離データ通信、あるいはＩＥＥＥ　８０２．１１に準拠した通信機器を小電力化して通信範囲を限定することによって、短時間のうちに２つの機器で発生する物理的なアクセスを代用することもできる。

【００６３】

以下、図面を参照しながら本発明の実施形態について詳解する。

【００６４】

図４には、本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示している。

【００６５】

家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどＷＡＮ、あるいは他のＬＡＮに接続されている。ホーム・ネットワークのｄｅｆａｕｌｔ　Ｇａｔｅｗａｙはホーム・ルータに設定されている。

【００６６】

ホーム・ネットワークは、例えばハブ（集結装置）にホーム・サーバやクライアント端末などの２以上のホスト装置のＬＡＮケーブルを接続することにより構成される。

【００６７】

ホーム・サーバやクライアント端末、ホーム・ルータなどのホーム・ネットワーク上のホスト装置、並びに外部ネットワーク上のホスト装置は、機器固有のＭＡＣアドレスを有している。ホスト装置は、受信先ＭＡＣアドレス及び送信元ＭＡＣアドレスを含んだヘッダ情報を持つパケット、例えばイーサネット（登録商標）フレームを、ネットワーク経由で送受信する。

【００６８】

ホーム・サーバやクライアント端末などのホーム・ネットワーク上のホスト装置は、例えばＵＰｎＰ対応機器として構成される。この場合、ネットワークに対する接続機器の追加や削除が容易である。ホーム・ネットワークに新たに接続する機器は、以下の手順に従って、コンテンツ利用などホーム・ネットワーク上のサービスを享受することができるようになる。

【００６９】

（１）アドレッシング処理：ＩＰアドレスなどの自己のデバイスＩＤを取得する

（２）ディスカバリ処理：ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する

（３）サービス要求処理：ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

【００７０】

ホーム・ネットワーク上では、個人的又は家庭の範囲内での使用であると推定されるローカル環境が形成されている。したがって、ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツ

を取得し、蓄積し、家庭内でコンテンツを配信する。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用することが許容される。

【００７１】

ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

【００７２】

また、図５には、本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示している。

【００７３】

ホーム・ネットワークは、ホーム・ルータ経由でインターネットなどＷＡＮ、あるいは他のＬＡＮに接続されている。この場合も、ホーム・ネットワークのｄｅｆａｕｌｔ　Ｇａｔｅｗａｙはホーム・ルータに設定されている。

【００７４】

図４との相違は、ホーム・ネットワーク上に２台のホーム・サーバが存在する点である。各ホーム・サーバは、ホーム・ネットワーク上に同時に存在してもよいし、あるいは時間差を以って接続されてもよい。

【００７５】

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、これらをメンバー登録してグループを形成し、コンテンツ配信並びコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。また、クライアント端末は、同じホーム・ネットワーク上の２台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

【００７６】

図６には、サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示している。

【００７７】

このシステムは、プロセッサ１０を中心に構成されている。プロセッサ１０は、メモリに記憶されたプログラムに基づいて各種の処理を実行する。また、プロセッサは、バス３０を介して接続されている各種の周辺機器を制御している。バス３０に接続された周辺機器は次のようなものである。

【００７８】

メモリ２０は、例えばＤＲＡＭ（Ｄｙｎａｍｉｃ　ＲＡＭ）などの半導体メモリで構成され、プロセッサ１０において実行されるプログラム・コードをロードしたり、実行プログラムの作業データを一時格納したりするために使用される。

【００７９】

ディスプレイ・コントローラ２１は、プロセッサ１０から送られてくる描画命令に従って表示画像を生成し、表示装置２２に送る。ディスプレイ・コントローラに接続された表示装置２２は、ディスプレイ・コントローラ２１から送られた表示画像情報に従い、その画像を画面に表示出力する。

【００８０】

入出力インターフェース２３は、キーボード２４やマウス２５が接続されており、キーボード２４やマウス２５からの入力信号をプロセッサ１０へ転送する。

【００８１】

ネットワーク・インターフェース２６は、ＬＡＮやインターネットなどの外部ネットワークに接続されており、インターネットを介したデータ通信を制御する。すなわち、プロセッサ１０から送られたデータをインターネット上の他の装置へ転送するとともに、インターネットを介して送られてきたデータを受け取りプロセッサ１０に渡す。

【００８２】

ハード・ディスク装置（ＨＤＤ：Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）コントローラ２７には、ＨＤＤなどの大容量外部記憶装置２８が接続されており、ＨＤＤコントローラ２７が接続されたＨＤＤ２８へのデータの入出力を制御する。ＨＤ

Ｄ２８には、プロセッサが実行すべきオペレーティング・システム（ＯＳ）のプログラム、アプリケーション・プログラム、ドライバ・プログラムなどが格納されている。アプリケーション・プログラムは、例えば、ホーム・サーバとしてホーム・ネットワーク上の各クライアント端末の認証処理を行なったり、コンテンツの提供やライセンスの発行を行なったりするサーバ・アプリケーションや、サーバから提供されたコンテンツの再生などコンテンツの利用を行なうクライアント・アプリケーションなどである。

【００８３】

仲介装置インターフェース４０は、ローカル環境にある他の機器との間で、短い時間内で同じ仲介装置への物理アクセスを共有するための装置である。仲介装置としては、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）やメモリ・スティックなどの標準的にインターフェースを介して機器へ装着される記憶媒体、非接触ＩＣカードなどが挙げられる。前者の場合、仲介装置インターフェース４０はメディア・スロットであり、後者の場合はカード読み書き装置となる。

【００８４】

同じ仲介装置に対するアクセスが比較的短時間のうちに収容されている機器同士は、至近距離すなわち同じ家庭内に配置されていると推定されることから、ローカル環境にあり、コンテンツを複製しても個人的又は家庭の範囲内での使用であるとされる。

【００８５】

なお、ホスト装置を構成するためには、図６に示した以外にも多くの電気回路などが必要である。但し、これらは当業者には周知であり、また、本発明の要旨を構成するものではないので、本明細書中では省略している。また、図面の錯綜を回避するため、図中の各ハードウェア・ブロック間の接続も一部しか図示していない点を了承されたい。

【００８６】

図７には、ネットワーク接続される２台のホスト装置間で、仲介装置を利用してローカル環境の認証を行なう様子を図解している。

【００８７】

ホスト装置は、コンテンツを配信するホーム・サーバとコンテンツを利用するクライアント端末であり、これらは同じホーム・ネットワーク、あるいはＷＡＮやその他のＬＡＮを経由して相互接続されている。

【００８８】

説明の便宜上、仲介装置はＵＳＢ接続メモリ・デバイスであり、仲介装置インターフェース４０は各ホスト装置に標準的に装備されているＵＳＢポートであるとする。

【００８９】

各ホスト装置がローカル環境すなわち同じ家庭内に配置されていれば、一方のホスト装置にＵＳＢ接続メモリを装着し、さらにこれを抜き取って他方のホスト装置に装着するという動作を、数十秒又は数分という比較的短い時間内に完了させることができる。そして、各ホスト装置がＵＳＢ接続メモリから読み取った識別情報をネットワーク経由で照合することにより、お互いに同じ仲介装置に物理アクセスしたことを確認することができる。このように短時間のうちに仲介装置を交換し合える至近距離でコンテンツを共有しても、著作権の保護範囲を逸脱しないと思料される。

【００９０】

ホスト装置＃１は、ＵＳＢ接続メモリが仲介装置インターフェースに装着されると、そこから識別情報を読み取るとともに、読み取った時刻を保持しておく。そして、ＵＳＢ接続メモリがホスト装置＃１から抜き取られて、今度はホスト装置＃２の仲介装置に装着される。ホスト装置＃２においても、ＵＳＢ接続メモリから識別情報を読み取るとともに、読み取った時刻を保持しておく。さらに、ホスト装置＃１とホスト装置＃２は、ネットワーク経由で通信して、互いに同じ識別情報を共有していることと、識別情報を取得した時刻が所定時間内であること（あるいは、識別情報を取得してから所定時間内に照合できたこと）を以って、両装置は至近距離すなわちローカル環境に置かれていることを確認する。

【００９１】

このようにして形成されたローカル環境内においてのみ、機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することがで

きる。

【００９２】

図７に示した例では、２台のホスト装置間でローカル環境の認証手続を行なっているが、勿論、３台以上のホスト装置であっても、ＵＳＢ接続メモリなどの仲介装置を介した照合処理を所定時間内に実現することができれば、すべての装置が同じローカル環境に置かれているものと推定して、グルーピングしてコンテンツを利用することができる。但し、無制限にグループ化を認めると、コンテンツが拡散してしまい著作権を保護できなくなる可能性があるので、一定の台数制限を設けるべきである。

【００９３】

図８には、ネットワーク接続される２台のホスト装置間で仲介装置を利用してローカル環境の認証を行なう変形例を図解している。

【００９４】

図７に示した例では、ＵＳＢ接続メモリには外部アクセスからの保護は施されていないので、同じ識別情報を持つＵＳＢ接続メモリを複製することにより、現実にはリモート環境にあるホスト装置間で同様の認証手続をなりすますことができてしまう。

【００９５】

これに対し、図８に示す例では、各ホスト装置の仲介装置インターフェース４０並びに仲介装置は耐タンパ性があり、外部からの不正アクセスから保護されている。また、仲介装置としてのＵＳＢ接続メモリには固定的な識別情報は格納されていない。

【００９６】

一方のホスト装置の仲介装置インターフェース４０－１は、乱数発生器を備えており、ＵＳＢ接続メモリが装着されると、メモリ内の耐タンパ性のある領域内に発生した乱数を書き込む。そして、仲介装置インターフェース４０－１は、発生した乱数を、至近距離内でＵＳＢ接続メモリを交換するに必要な短時間だけ保持しておく。

【００９７】

図９には、このときの仲介装置インターフェース４０－１と仲介装置の間で行なわれる動作を示している。ローカル環境の確認要求が発生すると、まず、仲介装置インターフェース４０－１と仲介装置の間で所定の認証処理が行なわれた後、仲介装置インターフェース４０－１は識別情報（例えば、一時的に発生した乱数）を仲介装置に転送する。これに対し、仲介装置はレスポンスを返す。

【００９８】

その後、ユーザは、ＵＳＢ接続メモリを抜き取って、他方のホスト装置の仲介装置インターフェース４０－２に装着する。仲介装置インターフェース４０－２は、ＵＳＢ接続メモリにアクセスして、書き込まれている乱数を読み取る。

【００９９】

図１０には、このときの仲介装置インターフェース４０－２と仲介装置の間で行なわれる動作を示している。ローカル環境の確認要求が発生すると、まず、仲介装置インターフェース４０－２と仲介装置の間で所定の認証処理が行なわれた後、仲介装置インターフェース４０－２は、仲介装置に対して識別情報（例えば、一時的に発生した乱数）を要求する。これに対し、仲介装置は仲介装置インターフェース４０－２にレスポンスを返す。

【０１００】

その後、各ホスト装置が乱数をネットワーク経由で照合することにより、お互いに同じ仲介装置に物理アクセスしたことを所定時間内に確認することができる。各ホスト装置がお互いの仲介装置への物理アクセスが所定時間内であったかどうかを確認するには、例えば各ホスト装置が仲介装置へアクセスした時刻を記憶しておき、それぞれのアクセス時刻を比較する方法、又は、乱数を発生したホスト装置が所定時間後に乱数を消失させるようにし、乱数が失われるまでにホスト装置間で同じ乱数を共有していることをネットワーク経由で確認する方法などを採ることができる。

【０１０１】

図１１には、ホスト装置＃１とホスト装置＃２の間で、ローカル環境の確認処理を行なう動作を示している。ホスト装置＃２は、ＵＳＢ接続メモリからセキュアに乱数を受け取ると、自己が接続されているＬＡＮセグメント上で同じ乱数を

保持しているホスト装置を探索する。この探索は、例えば、ＬＡＮ上で乱数を含んだローカル環境確認要求パケットをブロードキャストすることにより行なわれる。そして、ホスト装置＃１は、乱数を発生してから所定時間内、あるいは自己が発生した乱数を消失する前に同じ乱数を含んだパケットを受信すると、これに対しレスポンスを返す。これによって、ホスト装置＃１とホスト装置＃２は互いにローカル環境に置かれていることを確認する。

【０１０２】

このようにして形成されたローカル環境内においてのみ、機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

【０１０３】

このように短時間のうちに仲介装置を交換し合える至近距離でコンテンツを共有しても、著作権の保護範囲を逸脱しないと思料される。その後、ＵＳＢ接続メモリを介して交換した乱数を種情報として暗号キーを生成し、暗号化通信を行なうようにしてもよい。

【０１０４】

図８に示した例では、２台のホスト装置間でローカル環境の認証手続を行なっているが、勿論、３台以上のホスト装置であっても、ＵＳＢ接続メモリなどの仲介装置を介した照合処理を所定時間内に実現することができれば、すべての装置が同じローカル環境に置かれているものと推定して、グルーピングしてコンテンツを利用することができる。但し、無制限にグループ化を認めると、コンテンツが拡散してしまい著作権を保護できなくなる可能性があるので、一定の台数制限を設けるべきである。

【０１０５】

［追補］

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を

判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１０６】

【発明の効果】

以上詳記したように、本発明によれば、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で接続される機器同士の真正性を好適に認証することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することができる。

【０１０７】

また、本発明によれば、一方の機器において正当に取得されているコンテンツを他方の機器が著作権法で認められる私的使用の範囲内で利用できるかどうかを好適に認証することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することができる。

【０１０８】

本発明によれば、ローカル環境内においてのみ機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

【図面の簡単な説明】

【図１】

ホーム・ネットワークの基本構成を模式的に示した図である。

【図２】

２台のホーム・サーバが存在するホーム・ネットワークの構成例を示した図である。

【図３】

クライアント端末が複数のホーム・ネットワークに跨って接続する様子を示した図である。

【図４】

本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示した図である。

【図５】

本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示した図

である。

【図６】

サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示した図である。

【図７】

ネットワーク接続される２台のホスト装置間で、仲介装置を利用してローカル環境の認証を行なう様子を示した図である。

【図８】

図７に示したホスト装置間で行なうローカル環境の認証処理の変形例を示した図である。

【図９】

仲介装置インターフェース４０－１と仲介装置の間で行なわれる動作シーケンスを示した図である。

【図１０】

仲介装置インターフェース４０－２と仲介装置の間で行なわれる動作シーケンスを示した図である。

【図１１】

ホスト装置＃１とホスト装置＃２の間で、ローカル環境の確認処理を行なう動作を示した図である。

【符号の説明】

１０…プロセッサ

２０…メモリ

２１…ディスプレイ・コントローラ

２２…表示装置

２３…入出力インターフェース

２４…キーボード

２５…マウス

２６…ネットワーク・インターフェース

２７…ハード・ディスク装置コントローラ

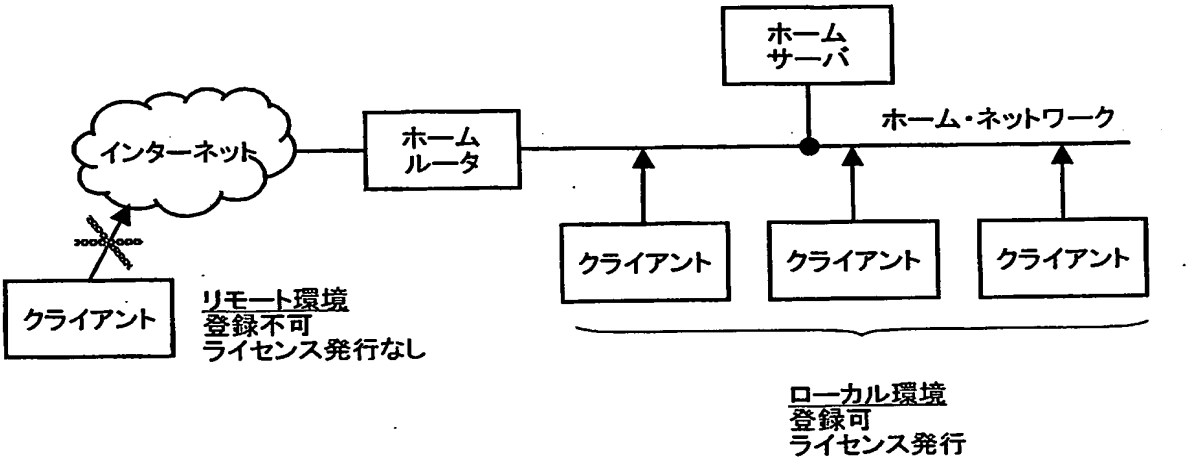
２８…ＨＤＤ

３０…バス

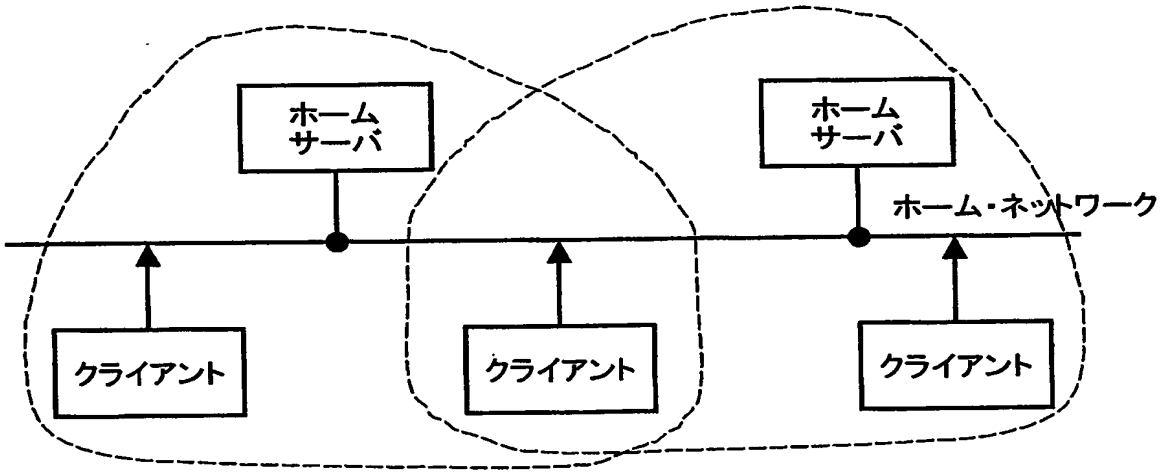
４０…仲介装置インターフェース

【書類名】　図面

【図１】

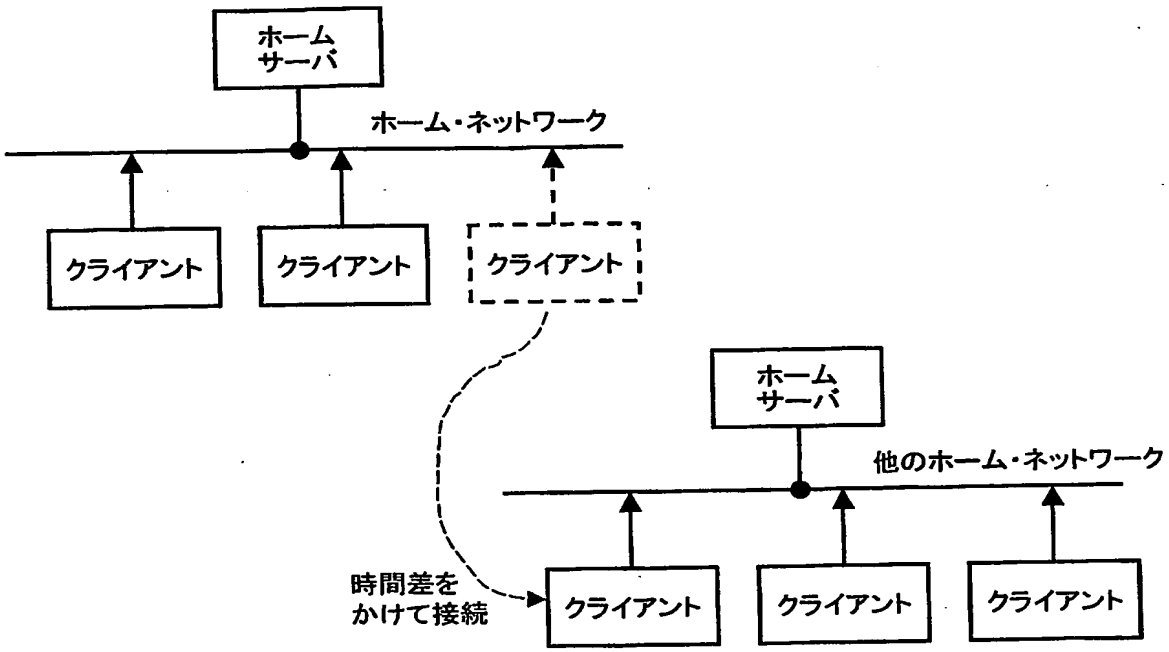



【図２】

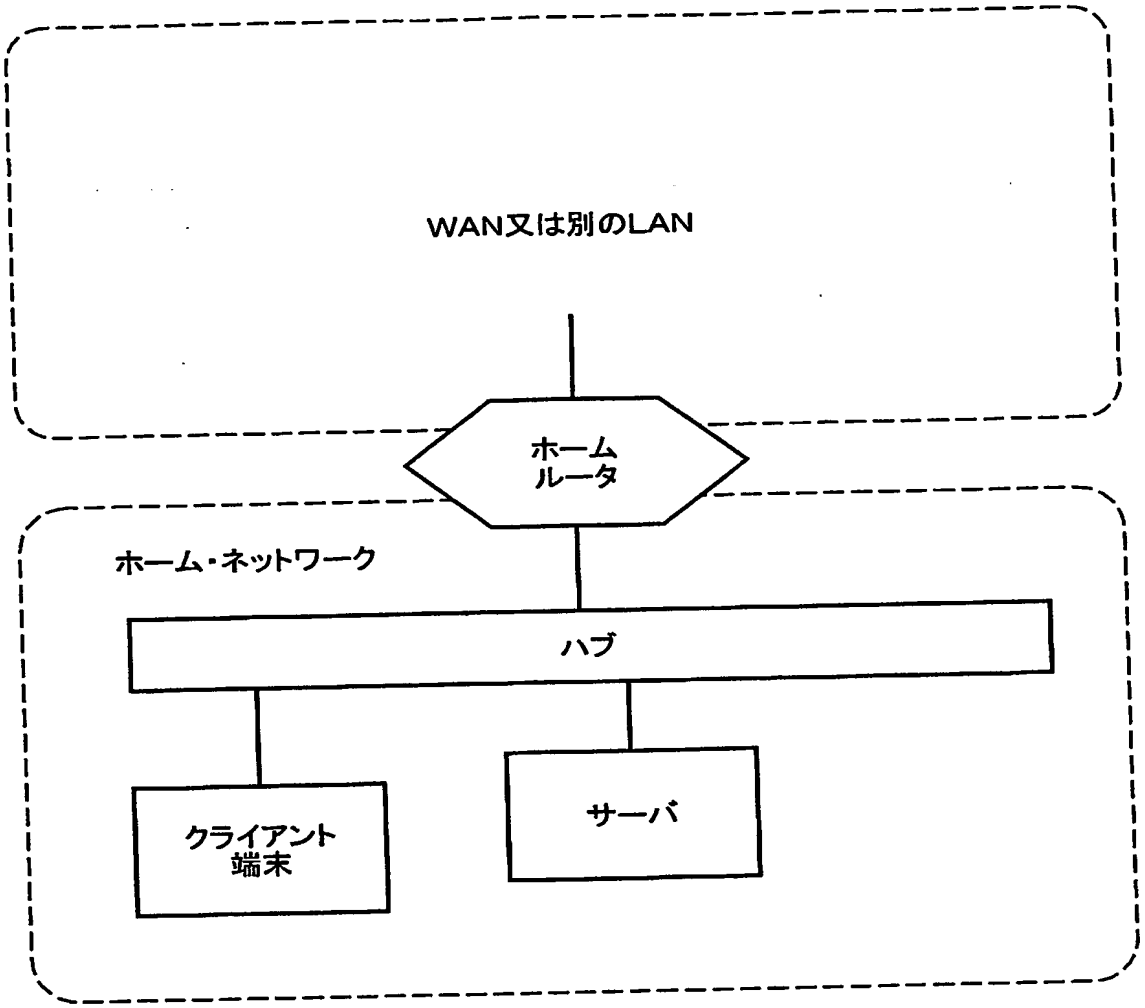



2台のホーム・サーバ
に同時に登録可

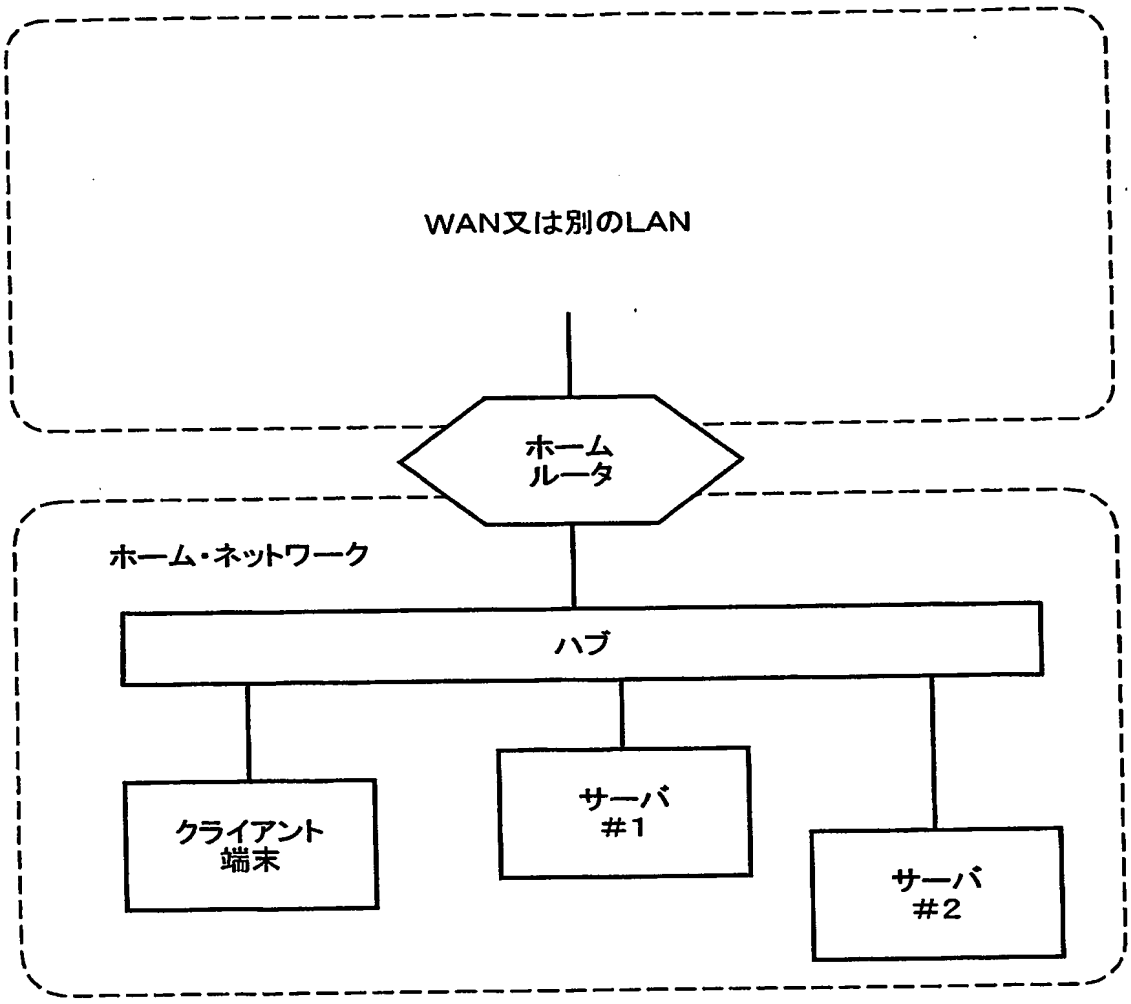
【図３】


ホーム
サーバ
ホーム・ネットワーク
クライアント
クライアント
クライアント
ホーム
サーバ
他のホーム・ネットワーク
時間差を
かけて接続
クライアント
クライアント
クライアント

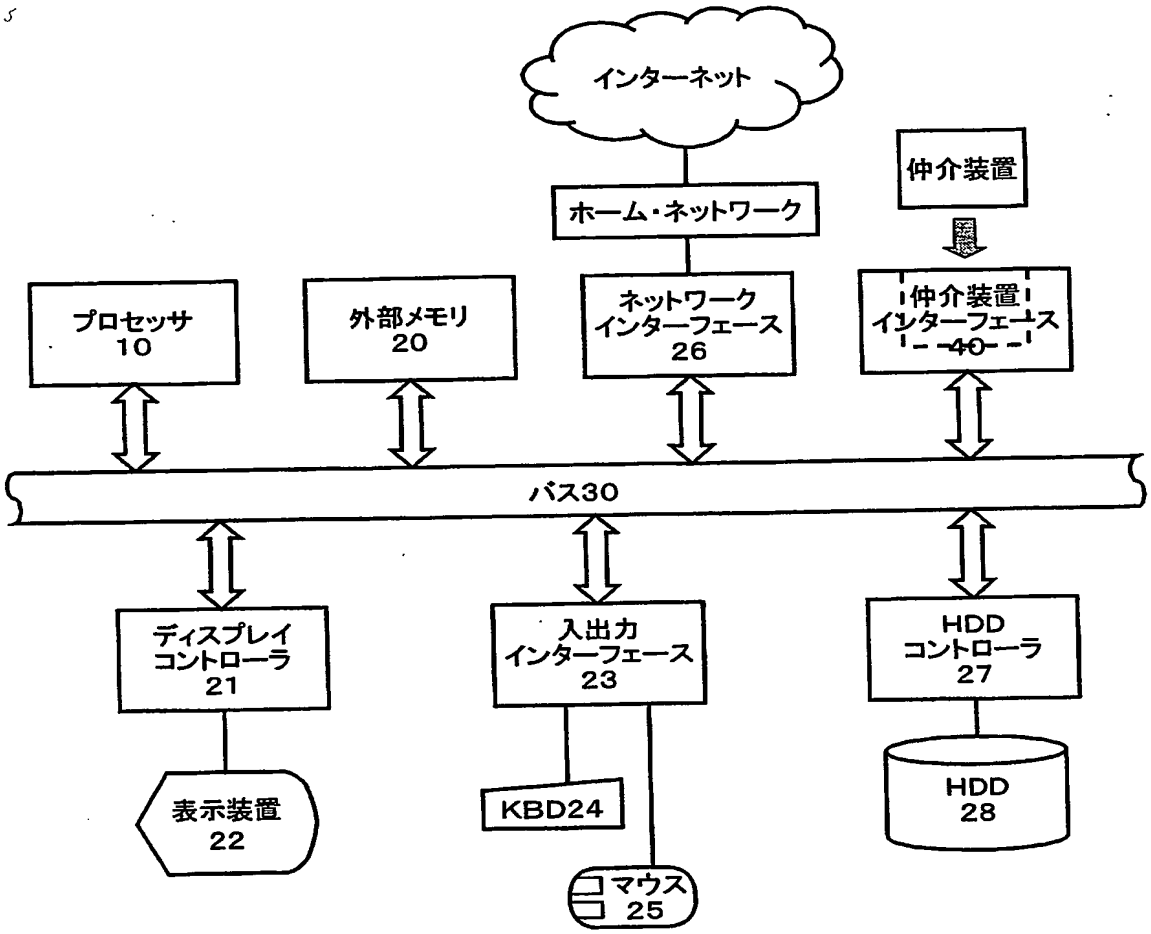
【図４】



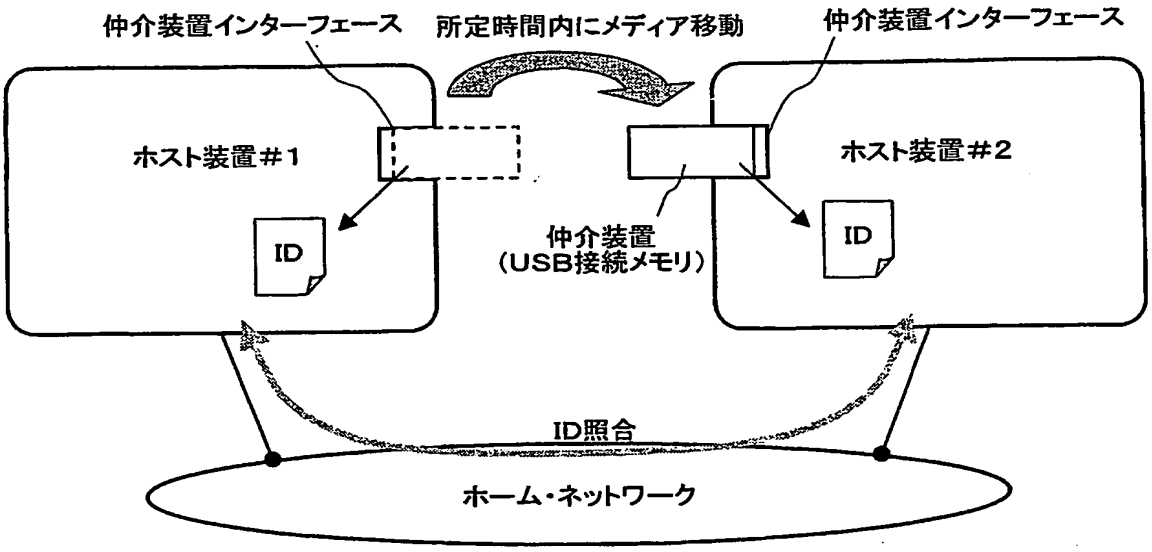
【図５】



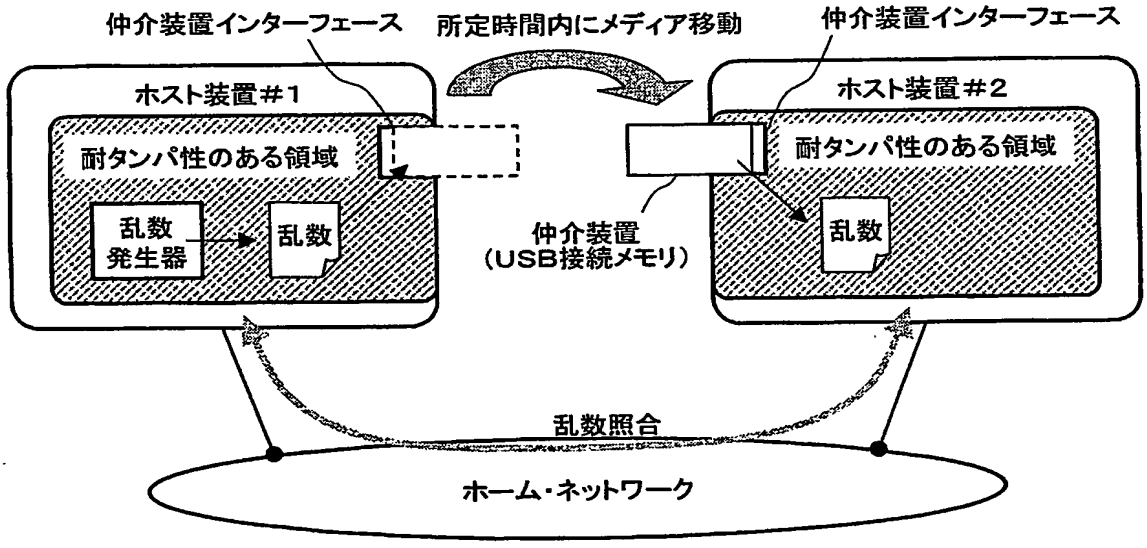
【図６】


インターネット
仲介装置
ホーム・ネットワーク
プロセッサ
10
外部メモリ
20
ネットワーク
インターフェース
26
仲介装置
インターフェース
40
バス30
ディスプレイ
コントローラ
21
入出力
インターフェース
23
HDD
コントローラ
27
表示装置
22
KBD24
マウス
25
HDD
28

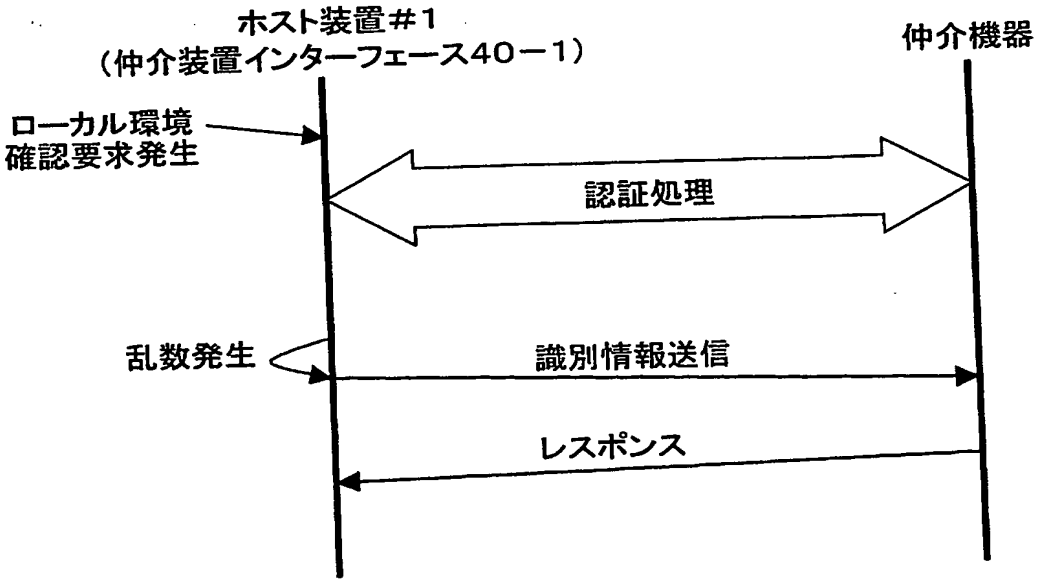
【図７】


仲介装置インターフェース
所定時間内にメディア移動
仲介装置インターフェース
ホスト装置＃1
ホスト装置＃2
ID
仲介装置
（USB接続メモリ）
ID
ID照合
ホーム・ネットワーク

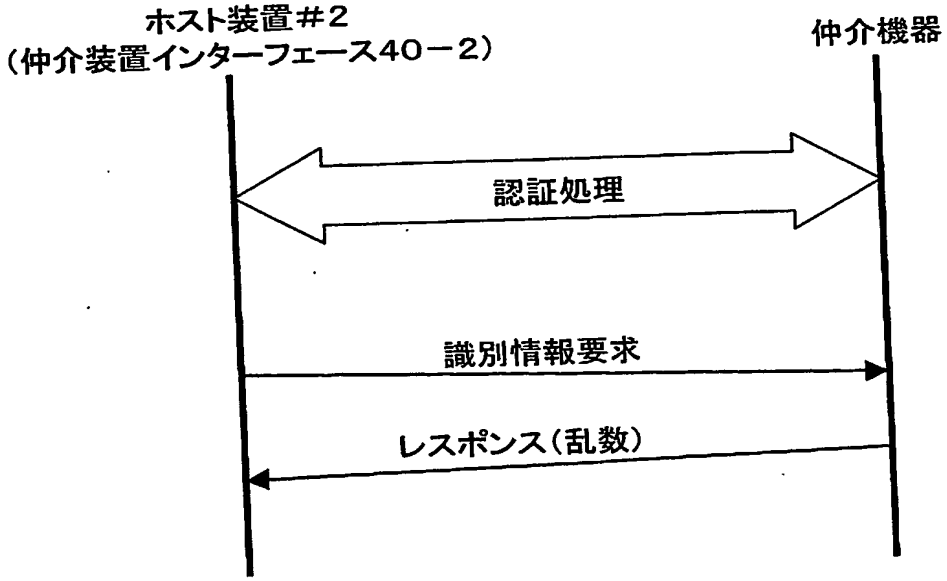
【図８】


仲介装置インターフェース
所定時間内にメディア移動
仲介装置インターフェース
ホスト装置＃1
ホスト装置＃2
耐タンパ性のある領域
耐タンパ性のある領域
乱数
発生器
乱数
仲介装置
（USB接続メモリ）
乱数
乱数照合
ホーム・ネットワーク

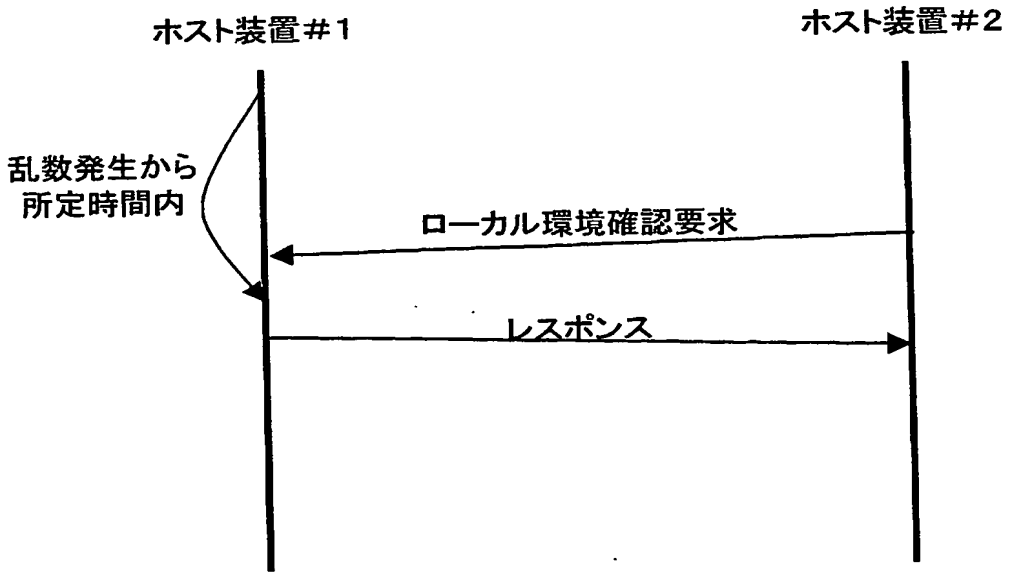
【図９】


ホスト装置＃１
（仲介装置インターフェース４０－１）
仲介機器
ローカル環境
確認要求発生
認証処理
乱数発生
識別情報送信
レスポンス

【図１０】



【図１１】



【書類名】　要約書

【要約】

【課題】　ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で接続される機器同士の真正性を認証する。

【解決手段】　ホーム・ネットワーク上に接続されている機器は、家庭内すなわち至近距離に位置し、ユーザは比較的短い時間のうちに互いの機器に物理的にアクセスすることができることを鑑み、コンテンツを配信するホーム・サーバとコンテンツを利用するクライアント端末が短い時間内で同じ物理媒体へのアクセスを共有することができたかどうかにより、同じホーム・ネットワークに接続されているかどうかを識別する。

【選択図】　図１

特願２００３－１３２９０２

# 出願人履歴情報

識別番号 [０００００２１８５]

１．変更年月日 １９９０年 ８月３０日
[変更理由] 新規登録
住所 東京都品川区北品川６丁目７番３５号
氏名 ソニー株式会社